(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－307603
（P2000－307603A）
(43)公開日　平成12年11月２日(2000.11.2)

| (51)Int.Cl.' | 識別記号 | ＦＩ | | テーマコード'(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ　12/28 | | Ｈ０４Ｌ　11/00 | ３１０Ｄ | ５Ｋ０３０ |
| 12/24 | | 11/08 | | ５Ｋ０３３ |
| 12/26 | | | | |

審査請求　未請求　請求項の数27　ＯＬ　（全 22 頁）

(21)出願番号　特願平11－117197

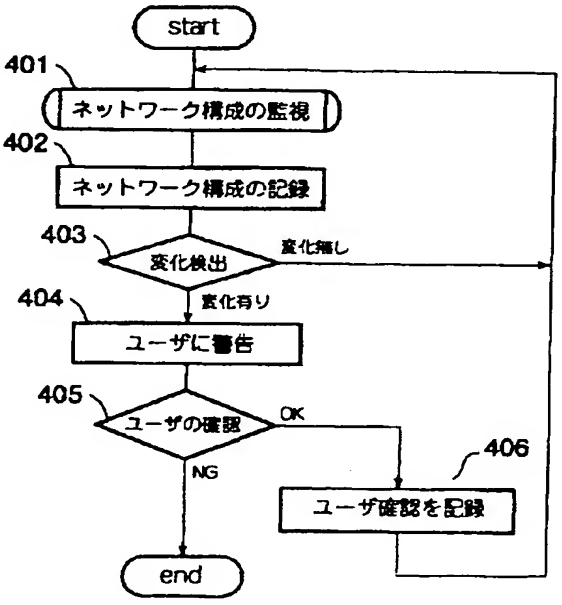
(22)出願日　平成11年４月23日(1999.4.23)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　佐々木　雄飛
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内
(72)発明者　篠原　利章
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内
(74)代理人　100082692
弁理士　蔵合　正博

最終頁に続く

(54)【発明の名称】　ネットワーク監視方法および装置

(57)【要約】
【課題】　ＩＥＥＥ１３９４ネットワークに代表される活線接続可能なネットワークにおいて、ネットワークに不正に接続された機器を発見することでセキュリティを保つことを目的とする。
【解決手段】　ネットワークトポロジを監視、記録することまたは伝送遅延の変化を監視、記録することでトポロジの変化からネットワークに追加、削除された機器を発見し、機器固有の情報またはバスリセット前情報で機器の認証を行なう。



【特許請求の範囲】

【請求項１】　ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することでネットワーク構成の変化を認識し、ネットワークに不正な機器が接続されるのを監視するネットワーク監視方法。

【請求項２】　ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワーク監視装置。

【請求項３】　各機器に接続状態を問い合わせることでネットワーク構成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することでネットワーク構成の変化を認識するネットワーク監視方法。

【請求項４】　各機器に接続状態を問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較する？ットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワークネットワーク監視装置。

【請求項５】　請求項１に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項６】　請求項２に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項７】　請求項３に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項８】　請求項４に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項９】　ネットワーク構成のリセット信号を検出し、ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することでネットワーク構成の変化を認識するネットワーク監視方法。

【請求項１０】　ネットワーク構成のリセット信号を検出するリセット検出部と、ネットワーク構成を知る機能のある機器に問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワーク監視装置。

【請求項１１】　ネットワーク構成のリセット信号後に発生するネットワーク上の機器の識別信号を受信することでネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することでネットワーク構成の変化を認識するネットワーク監視方法。

【請求項１２】　ネットワーク構成のリセット信号を検出するリセット検出部と、リセット後に発生するネットワーク上の機器の識別信号を受信することでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワーク監視装置。

【請求項１３】　請求項９に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項１４】　請求項１０に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項１５】　請求項１１に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項１６】　請求項１２に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項１７】　複数の手段でネットワーク構成を検出し、各手段から得られるネットワーク構成に矛盾が無いか判定するネットワーク監視方法。

【請求項１８】　複数の手段でネットワーク構成を検出するネットワーク構成検出部または複数のネットワーク構成検出部と、検出されたネットワーク構成を記録する記録部と、検出されたネットワーク構成に矛盾がないか調べる比較部とを具備することを特徴とするネットワー

ク監視装置。

【請求項１９】　自らネットワーク構成を知り、管理する能力を持ち、ネットワークを管理するマネージャとなり、マネージャになれなかった場合、監視者または上位のネットワーク監視装置に警告を発するネットワーク監視方法。

【請求項２０】　自らアイソクロナス転送とそのリソースを管理する能力を持ち、アイソクロナス転送を管理するマネージャとなり、マネージャになれなかった場合、監視者または上位のネットワーク監視装置に警告を発するネットワークネットワーク監視方法。

【請求項２１】　機器間の伝送遅延を観測し、記録し、観測結果と以前の観測結果の記録との差分を判定し、伝送遅延の変化を認識することでネットワーク構成の変化を認識するネットワーク監視方法。

【請求項２２】　機器間の伝送遅延を観測する伝送遅延検出部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項２３】　伝送遅延検出の条件を設定、記録する検出条件記録部と、伝送遅延測定用のパケットを送出するパケット送信部と、そのａｃｋを受信するパケット受信部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項２４】　ネットワーク上のデータパケットとそれに対するａｃｋを監視するパケット監視部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項２５】　複数の機器からなるネットワークシステムで、ネットワーク構成をリセットする信号の前に予め情報を交換しておき、リセット後に予め交換しておいた情報に基づく認証を行なうことで、リセット以前から存在した機器と新たに追加された機器および削除された機器を認識するネットワーク監視方法。

【請求項２６】　ネットワーク構成をリセットする信号の前に交換する情報を生成する鍵生成部と、リセット前情報を記録しておく記録部と、リセットを検出するリセット検出部と、予め交換しておいた情報に基づきリセット後に認証を行なう機器認証処理部とを具備することを特徴とするネットワーク監視装置。

【請求項２７】　請求項１から２６に記載のネットワーク監視方法およびネットワーク監視装置のいずれかを具備するネットワーク監視システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークのセキュリティに係り、特にＩＥＥＥ１３９４に代表される活線接続可能なネットワークにおける機器の不正接続に対するセキュリティに関する。

【０００２】

【従来の技術】ＩＥＥＥ１３９４は、シンプルな構成と高いパフォーマンスにより家庭内ＬＡＮなど今後の様々な機器間接続手段として期待されている。１００Ｍｂｐｓ以上の転送速度、Isochronous と呼ばれるマルチメディアデータ転送に適した転送方式、機器の接続を自動的に認識することでネットワークの稼働中に機器を追加、削除が可能な活線接続機能を備え、トゥリー型のネットワークを構成し、広い用途に活用することが可能である。

【０００３】用途のひとつにカメラを用いた監視システムを構成することが考えられる。これは、高速な転送速度のために多量の映像等のデータを伝送することが可能になるためである。従来の監視システムの場合、監視に必要な数のアナログ出力カメラとそれと同数のビデオキャプチャボード等のＡ／Ｄ変換機構を必要とし、また、カメラとビデオキャプチャボードとの接続に一本のケーブルを必要とし、カメラ台数と同じ本数のケーブルを引き回す必要があった。

【０００４】しかし、ＩＥＥＥ１３９４などの活線接続が可能なネットワークを利用した監視システムの場合、監視に必要な数のデジタル出力カメラに対し、ネットワーク監視装置として受信、記録のためのパソコンを最低ひとつ接続するだけで済み、またトゥリー型のネットワークを構成することにより、少ないケーブル本数で監視システムを構成することが可能である。

【０００５】

【発明が解決しようとする課題】活線接続が可能なネットワークでは、ネットワークに簡単に機器を接続することができる。これは便利な機能である反面、監視システムなどのセキュリティの必要とされるネットワークにおいては部外者に不正に機器を接続された場合、ネットワーク上の情報の盗聴、改ざん、不正なパケットの発信など重大な問題を引き起こす可能性がある。このためＩＥＥＥ１３９４などの活線接続が可能なネットワークにおいては、ネットワークに接続してくる機器を監視し、それが不正な機器であるか否かを判別し、不正な機器の接続を防止することでネットワーク自体をセキュアに保つことが望ましい。

【０００６】そこで本発明では、ネットワークへの機器の追加、削除およびネットワーク構成の変化を監視し、ネットワークへの不正な機器の接続を発見することのできるネットワーク監視方法および装置を提供することを

目的とする。

【０００７】

【課題を解決するための手段】原理的には、ネットワークのノードとなる機器がポート別に接続状態を把握可能であれば、ネットワーク構成を得ることができる。ＩＥＥＥ１３９４ネットワークでは、ひとつの機器が複数のポートを持つが、接続はポート毎に認識が可能である。これを利用するとネットワークの構成を知ることができる。

【０００８】活線接続可能なネットワークにおいては、機器をネットワークに接続、ネットワークから削除する際に、ネットワークを初期化し、機器のＩＤを決定する等の理由でネットワークにリセットを掛ける必要がある。リセット後には各機器の能力、状態を交換し、各機器のＩＤを決定しネットワーク構成を明らかにする。これらによりネットワーク構成を得ることができ、またネットワーク構成の変化を検出することができる。

【０００９】ＩＥＥＥ１３９４ネットワークでは、新しい機器が接続されたりすでに接続されている機器が削除されたりすると、バスリセットがかかり、ネットワーク構成の認識を始める。ＩＥＥＥ１３９４ネットワークのノードは、階層型の親子関係を持つ。バスリセット後は最初に親子関係を決定する。接続されたポートをひとつしか持たないノードはリーフと呼ばれ、自ら子ノードとなろうとし、接続されたポートに接続された隣接するノードに、自分は子ノードとなる旨伝達する。伝達を受けたノードは親ノードとなる。親ノードとなったノードは、ネットワークがトゥリー型であることが保証されているため、遅かれ早かれ（Ａ）接続されているノードすべてが子ノードになるか、あるいは（Ｂ）ひとつの接続されているノードを除いたすべての接続されているノードが子ノードとなる。（Ａ）の状況になった場合、そのノードはルートとなり、親子関係の構築は終了する。（Ｂ）の状況になった場合、そのノードは残された接続されたポートに接続された隣接するノードに自分は子ノードとなる旨伝達し、以後再帰的にルートが決定されるまで繰り返す。

【００１０】親子関係が決定すると、親子の序列上決められた順番に自己識別パケットと呼ばれるパケットをブロードキャストし、各ノードのＩＤを決定してゆく。全ノードのＩＤが決定すると、ネットワークの構築の終了であり、以後は普通にデータ伝送が行なわれる。自己識別パケットには、各ノードのポート毎の接続状態が記録されている。このパケットを、トポロジマップレジスタと呼ばれるレジスタを持った機器が収集し、ネットワーク構成を明らかにし、トポロジマップレジスタに格納する。ネットワーク上の機器は、トポロジマップレジスタを見ることによりネットワーク構成を知ることができる。また、ネットワーク監視装置が自ら自己識別パケットを収集し、ネットワーク構成を知ることもできる。

【００１１】以上述べたようにＩＥＥＥ１３９４では、ネットワーク構成を得ることが容易であり、ネットワーク構成の変化を監視することで不正な機器の接続が行なわれた可能性を検出することが可能になる。活線接続可能なネットワークにおいて、ネットワークを管理する機器は必ずしも一意に決定されるとは限らず、何らかの交渉を通じて管理者が決定することがある。この時、管理者を監視し、問題のある機器が管理者になることを防ぐ必要がある。

【００１２】ＩＥＥＥ１３９４では、バスマネージャはトポロジマップを持つことが保証されているが、バスマネージャは能力さえあれば成ることが可能なため、どの機器がバスマネージャになるかも監視する。また、バスマネージャを決定するのはアイソクロナスマネージャであるため、どの機器がアイソクロナスマネージャになるかも監視する。また、活線接続であることを利用し、自己識別パケットを偽る、あるいは出力しないノードが正常なノードの間に不正に接続される可能性がある。そこで伝送遅延を測定、記録し、変化を検出することで、不正なノードを検出する。また、ネットワーク構成が変化した際のリセットの前に適当な情報を共有しておき、リセット後にその情報を用いた認証を行なうことで、機器がリセット以前から存在したかどうかを検出することが可能となる。これらに通常の認証を加えて機器の正当性を確認することで、さらにネットワークのセキュアを高めることができる。

【００１３】

【発明の実施の形態】請求項１に記載のネットワーク監視方法は、ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することでネットワーク構成の変化を認識し、ネットワークに不正な機器が接続されるのを監視することを特徴とし、特別な手段を必要とせず、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することで、ネットワークをセキュアに保つことができるという作用を有する。

【００１４】請求項２に記載のネットワーク監視装置は、ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、監視機器にネットワーク構成検出能力を必要とせずにネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００１５】請求項３に記載のネットワーク監視方法は各機器に接続状態を問い合わせることでネットワーク構

成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することでネットワーク構成の変化を認識することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００１６】請求項４に記載のネットワーク監視装置は各機器に接続状態を問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００１７】請求項５に記載のネットワーク監視方法は、請求項１に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別することを特徴とし、特別な手段を必要とせず、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００１８】請求項６に記載のネットワーク監視装置は、請求項２に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、特別な手段を必要とせず、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００１９】請求項７に記載のネットワーク監視方法は、請求項３に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００２０】請求項８に記載のネットワーク監視装置は、請求項４に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００２１】請求項９に記載のネットワーク監視方法は、ネットワーク構成のリセット信号を検出し、ネットワーク構成を知る機能のある機器に問い合わせることでネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することでネットワーク構成の変化を認識することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００２２】請求項１０に記載のネットワーク監視装置は　ネットワーク構成のリセット信号を検出するリセット検出部と、ネットワーク構成を知る機能のある機器に問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００２３】請求項１１に記載のネットワーク監視方法は、ネットワーク構成のリセット信号後に発生するネットワーク上の機器の識別信号を受信することでネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することでネットワーク構成の変化を認識することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００２４】請求項１２に記載のネットワーク監視装置は、ネットワーク構成のリセット信号を検出するリセット検出部と、リセット後に発生するネットワーク上の機器の識別信号を受信することでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００２５】請求項１３に記載のネットワーク監視方法は、請求項９に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワ

ークがセキュアか否かを自動的に判別することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００２６】請求項１４に記載のネットワーク監視装置は、請求項１０に記載のネットワークネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００２７】請求項１５に記載のネットワーク監視方法は、請求項１１に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００２８】請求項１６に記載のネットワーク監視装置は、請求項１２に記載のネットワークネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断することができるという作用を有する。

【００２９】請求項１７に記載のネットワーク監視方法は、複数の手段でネットワーク構成を検出し、各手段から得られるネットワーク構成に矛盾が無いか判定することを特徴とし、フォールトトレランスを維持することができ、また、不正なトポロジマップを検出することでネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００３０】請求項１８に記載のネットワーク監視装置は、複数の手段でネットワーク構成を検出するネットワーク構成検出部または複数のネットワーク構成検出部と、検出されたネットワーク構成を記録する記録部と、検出されたネットワーク構成に矛盾がないか調べる比較部とを具備することを特徴とし、ネットワーク構成獲得手段を複数持つことでフォールトトレランスを維持することができ、また、不正なネットワーク構成を報告したネットワーク構成獲得手段を検出することでネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００３１】請求項１９に記載のネットワーク監視方法は、自らネットワーク構成を知り、管理する能力を持ち、ネットワークを管理するマネージャとなり、マネージャになれなかった場合、監視者または上位のネットワーク監視装置に警告を発することを特徴とし、ネットワークを管理するマネージャの乗っ取りを防止するという作用を有する。

【００３２】請求項２０に記載のネットワーク監視方法は、自らアイソクロナス転送とそのリソースを管理する能力を持ち、アイソクロナス転送を管理するマネージャとなり、監視者または上位のネットワーク監視装置に警告を発することを特徴とし、アイソクロナス転送を管理するマネージャの乗っ取りを防止するという作用を有する。

【００３３】請求項２１に記載のネットワーク監視方法は、機器間の伝送遅延を観測し、記録し、観測結果と以前の観測結果の記録との差分を判定し伝送遅延の変化を認識することでネットワーク構成の変化を認識することを特徴とし、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【００３４】請求項２２に記載のネットワーク監視装置は、機器間の伝送遅延を観測する伝送遅延検出部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、ネットワークにノードとして振舞わない不正な機器の接続された可能性を検出することができるという作用を有する。

【００３５】請求項２３に記載のネットワーク監視装置は、伝送遅延検出の条件を設定、記録する検出条件記録部と、伝送遅延測定用のパケットを送出するパケット送信部と、そのａｃｋを受信するパケット受信部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、ネットワークにノードとして振舞わない不正な機器の接続された可能性を検出することができるという作用を有する。

【００３６】請求項２４に記載のネットワーク監視装置は、ネットワーク上のデータパケットとそれに対するａｃｋを監視するパケット監視部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変

化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、トラフィックを増加させることなく、ネットワークにノードとして振舞わない不正な機器の接続された可能性を検出することができるという作用を有する。

【００３７】請求項２５に記載のネットワーク監視方法は、複数の機器からなるネットワークシステムで、ネットワーク構成をリセットする信号の前に予め情報を交換しておき、リセット後に予め交換しておいた情報に基づく認証を行なうことで、リセット以前から存在した機器と新たに追加された機器および削除された機器を認識することを特徴とし、リセット以前から存在する機器を識別し、ネットワークに新たに接続された不正な機器を発見することができるという作用を有する。

【００３８】請求項２６に記載のネットワーク監視装置は、ネットワーク構成をリセットする信号の前に交換する情報を生成する鍵生成部と、リセット前情報を記録しておく記録部と、リセットを検出するリセット検出部と、予め交換しておいた情報に基づきバスリセット後に認証を行なう機器認証処理部とを具備することを特徴とし、リセット以前から存在する機器を識別し、ネットワークに新たに接続された不正な機器を発見することができるという作用を有する。

【００３９】請求項２７に記載のネットワーク監視システムは、請求項１から２６に記載のネットワーク監視方法およびネットワーク監視装置のいずれかを具備することを特徴とし、ネットワークをセキュアに保つことで安全にネットワーク上でデータの送受信をすることが可能であるという作用を有する。

【００４０】以下、添付図面の図１から２０に基づき、本発明の実施の形態を詳細に説明する。なお、ここでは活線接続可能なネットワークとしてＩＥＥＥ１３９４ネットワークの場合を想定して説明している。また、以下の説明において、ネットワーク構成とは、どの機器の何番のポートにどの機器の何番のポートが接続されているかという情報であり、ネットワーク構成を検出するとは、ここではネットワーク内のノードとアークの関係を把握することを指す。ネットワーク構成の検出の手段としては、バスマネージャなどの物理層でトポロジマップを持つ機器に問い合わせを行なう、機器に接続状態を問い合わせる、自らバスマネージャになる、等の方法がある。

【００４１】トポロジマップを持つ機器に問い合わせる方法は、ネットワーク監視装置に特別な能力が無くともネットワーク構成を知ることができるという作用がある。機器に接続状態を問い合わせる方法は、物理層に直接アクセスすること無しにネットワーク構成を知ることができ、またネットワーク構成情報以外の情報も同時に扱うことができるという作用がある。ネットワーク監視装置自らがバスマネージャになる場合、自分以外の機器がバスマネージャに決定したか、あるいは自分以外の機器がバスマネージャに立候補したかという情報をセキュリティの判断に用いることができる。この情報を得ることは、バスマネージャになりすまそうとする不正な機器を発見することができるという作用を有する。自らバスマネージャにならない場合、バスマネージャを決定するアイソクロナスマネージャに自らがなっても良い。この時、自分以外の機器がアイソクロンナスマネージャに決定したか、あるいは自分以外の機器がアイソクロナスマネージャに立候補したか、あるいは自分がバスマネージャに決定した機器以外の機器がバスマネージャに立候補したかという情報をセキュリティの判断に用いることができる。この情報を得ることは、アイソクロナスマネージャまたはバスマネージャになりすまそうとする不正な機器を発見することができるという作用を有する。

【００４２】セキュアなネットワーク構成の条件としては、セキュアなネットワーク構成のリスト、ネットワークに接続が許容されている機器と接続位置のリスト、許容されている機器の組、許容されている機器間のアークのトポロジ、許されるネットワーク構成変化のリスト、あるいはこれらを論理的に記述した式等、あるいはこれらの組合せが用いられる。

【００４３】（実施の形態１）図１は本発明の実施の形態１におけるネットワーク監視方法を説明する図である。図１において、３０１ａ～３０１ｄはネットワークを構成するカメラ、３０８はネットワーク監視装置、３１１はネットワーク監視装置に登録されている機器およびネットワークの登録リストである。

【００４４】次に、図１を参照して本発明の実施の形態１におけるネットワーク監視方法を説明する。ネットワーク監視装置３０８は、ネットワーク構成を獲得する能力があり、また、ネットワーク機器についての固有な情報を得る手段を持っている。ここでは情報として機器のＩＤとして製造元および製造番号を用いる場合を説明する。ネットワーク監視装置３０８は、許容されるネットワーク機器およびネットワーク構成を登録する登録リスト３１１を持つ。登録リスト３１１の内容は、事前に登録されても良いし、ネットワーク監視装置３０８が監視結果を記録して更新してもよい。ここでは、ネットワーク監視装置３０８、カメラ３０１ａ、カメラ３０１ｂ、カメラ３０１ｃからなるネットワークが登録リスト３１１に登録されている。現在のネットワーク上の機器およびネットワーク構成は登録リスト３１１の内容に合致するために許容される。

【００４５】ここでカメラ３０１ｄをネットワークに接続するとする。その場合、ネットワーク上のネットワーク機器およびネットワーク構成が変化する。ネットワーク監視装置３０８は、ネットワーク機器の情報およびネットワーク構成を獲得し、それを登録リスト３１１と比較する。ネットワーク機器の情報およびネットワーク構

成が登録リスト３１１の内容と合致しない場合、ネットワーク監視装置３０８は警告を発する。

【００４６】本発明の実施の形態１におけるネットワーク監視方法を以上のように構成することにより、ネットワーク機器の情報およびネットワーク構成を利用し、ネットワークに不正な機器が接続された可能性を検出できるネットワーク監視方法を実現することができる。

【００４７】（実施の形態２）図２は本発明の実施の形態２におけるネットワーク監視方法の流れ図である。図２において、４０１はネットワーク構成の監視フェイズ、４０２はネットワーク構成の記録フェイズ、４０３はネットワーク構成の変化検出フェイズ、４０４はユーザに警告を行なうフェイズ、４０５はユーザの確認を受けるフェイズ、４０６はユーザの確認を受けたことを記録するフェイズである。

【００４８】次に、図２を参照して本発明の実施の形態２におけるネットワーク監視方法を説明する。監視者は設定された時刻にネットワーク構成を検出する（４０１）。検出時刻については、バスリセット直後、一定時間間隔、ランダム時間間隔、トラフィックの少ない時間、特定のイベントの直前または直後、ユーザの指示した時刻、常時、等の手段がある。検出されたネットワーク構成は記録される（４０２）。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成を比較される（４０３）。比較の結果、変化が認められなかった場合には４０１に戻り、次のネットワーク構成検出まで待機する。比較の結果変化が認められた場合、ユーザに警告を行なう（４０４）。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否か判断する。ユーザがセキュアであると判断した場合、その旨を記録し（４０６）、４０１に戻り、次のネットワーク構成検出まで待機する。

【００４９】なお、ユーザへの警告４０４は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告と共に行なっても良い。

【００５０】本発明の実施の形態２におけるネットワーク監視方法を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出できるネットワーク監視方法を実現することができる。

【００５１】（実施の形態３）図３は本発明の実施の形態３におけるネットワーク監視装置の構成を示すブロック図である。図３において、１０１はネットワーク、１０２はネットワーク構成を検出するネットワーク構成検出部、１０３はネットワーク構成を記録するネットワーク構成記録部、１０４はネットワーク構成の変化を検出するネットワーク構成変化検出部、１０５はネットワーク構成の変化を表示する表示部であり、１１０はユーザからの入力を受け付ける入力部である。

【００５２】次に、図３を参照して本発明の実施の形態３におけるネットワーク監視装置の動作を説明する。最初に、ネットワークがセキュアな状態において、ネットワーク構成検出部１０２は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部１０３は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、ネットワーク構成検出部１０２は、ネットワーク構成を検出する。ネットワーク構成変化検出部１０４は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、表示部１０５に変化を出力する。表示部１０５は、ネットワーク構成変化検出部１０４からの入力を受けて、それをユーザに対し表示する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部１０３は、新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。ユーザは、表示部１１０を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部１１０に入力する。ネットワーク構成記録部１０３は、入力部１１０からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。

【００５３】なお、表示部１１０の代わりに、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００５４】本発明の実施の形態３におけるネットワーク監視装置を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。

【００５５】（実施の形態４）図４は本発明の実施の形態４におけるネットワーク監視方法の流れ図であり、図２に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図４において、４０７は現在のネットワーク構成がセキュアであるという条件を新たに登録するフェイズ、４０８は登録されているセキュアなネットワーク構成の条件と現在のネットワークとを比較するフェイズ、４０９は比較結果、現在のネットワーク構成がセキュアか否かを判断するフェイズ、４１０はセキュアなネットワーク構成の条件を設定するフェイズである。

【００５６】次に、図４を参照して本発明の実施の形態

４におけるネットワーク監視方法を説明する。最初にネットワークがセキュアか否かを判断するための条件を設定する（４１０）。監視者は設定された時刻にネットワーク構成を検出する（４０１）。検出時刻については、バスリセット直後、一定時間間隔、ランダム時間間隔、トラフィックの少ない時間、特定のイベントの直前または直後、ユーザの指示した時刻、常時、等の手段がある。検出されたネットワーク構成は記録される（４０２）。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成を比較される（４０３）。比較の結果、変化が認められなかった場合には４０１に戻り、次のネットワーク構成検出まで待機する。比較の結果変化が認められた場合、検出された現在のネットワーク構成をセキュアなネットワーク構成の条件と比較し（４０８）、条件に合致するか否かを判断する（４０９）。現在のネットワーク構成がセキュアでなネットワーク構成の条件に合致した場合、４０１に戻り、次のネットワーク構成検出まで待機する。合致しなかった場合、ユーザに警告を行なう（４０４）。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否か判断する。ユーザがセキュアであると判断した場合、現在のネットワーク構成をセキュアなネットワーク構成の条件として新たに登録し（４０７）、４０１に戻り次のネットワーク構成検出まで待機する。

【００５７】なお、ユーザへの警告４０４は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００５８】本発明の実施の形態４におけるネットワーク監視方法を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出することとができ、与えられた条件に因ってネットワークがセキュアか否か自動的に判断するネットワーク監視方法を実現することができる。

【００５９】（実施の形態５）図５は本発明の実施の形態５におけるネットワーク監視装置の構成を示すブロック図であり、図３に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図５において、１０６は予めセキュアであるとされたネットワーク構成を記録しておく許容ネットワーク構成記録部、１０７はネットワーク構成が変化した場合にその新たなネットワーク構成はセキュアであるか否かを判断する判断部、１０８は変化した新たなネットワークがセキュアではないと判断された場合に警告を発する警告発生部である。

【００６０】次に、図５を参照して本発明の実施の形態５におけるネットワーク監視装置の動作を説明する。最初にユーザは、セキュアであると解っているネットワーク構成を許容ネットワーク構成記録部１０６に登録する。また、ネットワーク構成検出部１０２は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部１０３は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、ネットワーク構成検出部１０２は、ネットワーク構成を検出する。ネットワーク構成変化検出部１０４は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、判断部１０７に出力する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部１０３は、新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。判断部１０７は、ネットワーク構成変化検出部１０４からの入力を受けると、許容ネットワーク構成記録部１０６に記録されているセキュアと認定されているネットワーク構成と新たなネットワーク構成とを比較する。もし新たなネットワーク構成が、許容ネットワーク構成記録部１０６に記録されているセキュアと認定されているネットワーク構成に含まれる場合、判断部１０７は、ネットワーク構成記録部１０３に記録された新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。この時、判断部１０７は、変化があったことを警告発生部１０８に出力しても良い。もし新たなネットワーク構成が、許容ネットワーク構成記録部１０６に記録されているセキュアと認定されているネットワーク構成に含まれない場合、判断部１０７は、その旨を警告発生部１０８に出力する。警告発生部１０８は、判断部１０７からの入力を受け、ユーザに対し警告を発する。ユーザは表示部１０５を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部１１０に入力する。ネットワーク構成記録部１０３は入力部１１０からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。また、もしそのネットワーク構成がセキュアであった場合、ユーザは入力部１１０を介して許容ネットワーク構成記録部に新たなネットワーク構成を追加することもできる。

【００６１】なお、警告発生部１０８は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００６２】本発明の実施の形態５におけるネットワーク監視方法を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器

の接続された可能性を検出することとができ、与えられた条件に因ってネットワークがセキュアか否か自動的に判断するネットワーク監視方法を実現することができる。

【００６３】（実施の形態６）図６は本発明の実施の形態６におけるネットワーク監視装置の構成を示すブロック図である。これは図５の構成においてネットワーク構成記録部１０３とネットワーク構成変化検出部１０４とを省略した構成である。このような構成にした場合、実施の形態５の場合と比較して、ネットワーク構成が変化しない場合でも判断を行なわねばならず、判断部１０７の処理が多くなる一方、全体の構成が簡単になる。

【００６４】本発明の実施の形態６におけるネットワーク監視装置を以上のように構成することにより、簡易な構成で、ネットワーク構成の変化を検出し、予め与えられた情報を基にネットワークに不正な機器の接続された可能性を自動的に検出できるネットワーク監視装置を実現することができる。

【００６５】（実施の形態７）図７は本発明の実施の形態７におけるネットワーク監視方法の流れ図であり、図２に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図７において、４１１はバスリセット監視フェイズであり、４１２はバスリセットが起こったか否かを判断するフェイズである。

【００６６】次に、図７を参照して本発明の実施の形態７におけるネットワーク監視方法を説明する。監視者はバスリセットが発生しているか否かを検出する（４１１）。バスリセットが発生しない場合は待機する（４１２）。バスリセットが発生したら、ネットワーク構成を検出する（４０１）。検出されたネットワーク構成は記録される（４０２）。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成を比較される（４０３）。比較の結果変化が認められなかった場合には４１１に戻り、次のバスリセットが検出されるまで待機する。比較の結果、変化が認められた場合、ユーザに警告を行なう（４０４）。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否か判断する。ユーザがセキュアであると判断した場合、その旨を記録し（４０６）、４０１に戻り、次のバスリセットが検出されるまで待機する。

【００６７】なお、ユーザへの警告４０４は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００６８】本発明の実施の形態７におけるネットワーク監視方法を以上のように構成することにより、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否か自動的に判断するネットワーク監視方法を実現することができる。

【００６９】（実施の形態８）図８は本発明の実施の形態８におけるネットワーク監視装置の構成を示すブロック図であり、図３に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図８において、１０９はネットワークのバスリセットを検出するバスリセット検出部である。

【００７０】次に、図８を参照して本発明の実施の形態８におけるネットワーク監視装置の動作を説明する。最初に、ネットワークがセキュアな状態において、ネットワーク構成検出部１０２は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部１０３は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、バスリセット検出部１０９は、ネットワークのバスリセットを検出すると、その旨をネットワーク構成検出部１０２に出力する。ネットワーク構成検出部１０２は、それを受けてバスリセット後のネットワーク構成を検出する。ネットワーク構成変化検出部１０４は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、表示部１０５に変化を出力する。表示部１０５は、ネットワーク構成変化検出部１０４からの入力を受けて、それをユーザに対し表示する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部１０３は新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。ユーザは表示部１０５を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部１１０に入力する。ネットワーク構成記録部１０３は、入力部１１０からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。

【００７１】なお、表示部１０５の代わりに、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００７２】本発明の実施の形態８におけるネットワーク監視装置を以上のように構成することにより、バスリセットにともなうネットワーク構成の変化を最小の手順で検出し、ネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。

【００７３】（実施の形態９）図９は本発明の実施の形態９におけるネットワーク監視方法の流れ図であり、図４および図７に示す構成部の符号と同一の符号を有する

構成部は同様のため、説明を省略する。

【００７４】次に、図９を参照して本発明の実施の形態９におけるネットワーク監視方法を説明する。最初にネットワークがセキュアか否かを判断するための条件を設定する（４１０）。監視者はバスリセットが発生しているか否かを検出する（４１１）。バスリセットが発生しない場合は待機する（４１２）。バスリセットが発生したら、ネットワーク構成を検出する（４０１）。検出されたネットワーク構成は記録される（４０２）。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成を比較される（４０３）。比較の結果変化が認められなかった場合には４０１に戻り、次のネットワーク構成検出まで待機する。比較の結果変化が認められた場合、検出された現在のネットワーク構成をセキュアなネットワーク構成の条件と比較し（４０８）、条件に合致するか否かを判断する（４０９）。現在のネットワーク構成がセキュアでなネットワーク構成の条件に合致した場合、４１１に戻り、次のバスリセットが検出されるまで待機する。合致しなかった場合、ユーザに警告を行なう（４０４）。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否か判断する。ユーザがセキュアであると判断した場合、現在のネットワーク構成をセキュアなネットワーク構成の条件として新たに登録し（４０７）、４１１に戻り、次のバスリセットが検出されるまで待機する。

【００７５】なお、　ユーザへの警告４０４は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００７６】本発明の実施の形態９におけるネットワーク監視方法を以上のように構成することにより、最小の手順でネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出することとができ、与えられた条件に因ってネットワークがセキュアか否か自動的に判断するネットワーク監視方法を実現することができる。

【００７７】（実施の形態１０）図１０は本発明の実施の形態１０におけるネットワーク監視装置の構成を示すブロック図であり、図５および図８に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。

【００７８】次に、図１０を参照して本発明の実施の形態１０におけるネットワーク監視装置の動作を説明する。最初にユーザは、セキュアであると解っているネットワーク構成を許容ネットワーク構成記録部１０６に登録する。また、ネットワーク構成検出部１０２は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部１０３は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、バスリセット検出部１０９は、ネットワークのバスリセットを検出するとその旨をネットワーク構成検出部１０２に出力する。ネットワーク構成検出部１０２は、それを受けてバスリセット後のネットワーク構成を検出する。ネットワーク構成変化検出部１０４は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、判断部１０７に出力する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部１０３は、新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。判断部１０７は、ネットワーク構成変化検出部１０４からの入力を受けると、許容ネットワーク構成記録部１０６に記録されているセキュアと認定されているネットワーク構成と新たなネットワーク構成とを比較する。もし新たなネットワーク構成が、許容ネットワーク構成記録部１０６に記録されているセキュアと認定されているネットワーク構成に含まれる場合、判断部１０７は、ネットワーク構成記録部１０３に記録された新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。この時、判断部１０７は、変化があったことを警告発生部１０８に出力しても良い。もし新たなネットワーク構成が、許容ネットワーク構成記録部１０６に記録されているセキュアと認定されているネットワーク構成に含まれない場合、判断部１０７は、その旨を警告発生部１０８に出力する。警告発生部１０８は、判断部１０７からの入力を受け、ユーザに対し警告を発する。ユーザは表示部１０５を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部１１０に入力する。ネットワーク構成記録部１０３は、入力部１１０からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。また、もしそのネットワーク構成がセキュアであった場合、ユーザは入力部１１０を介して許容ネットワーク構成記録部１０６に新たなネットワーク構成を追加することもできる。

【００７９】なお、警告発生部１０８は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００８０】本発明の実施の形態１０におけるネットワーク監視装置を以上のように構成することにより、バスリセットにともなうネットワーク構成の変化を最小の手順で検出し、予め与えられた情報を基にネットワークに不正な機器の接続された可能性を自動的に検出できるネ

ットワーク監視装置を実現することができる。

【００８１】（実施の形態１１）図１１は本発明の実施の形態１１におけるネットワーク監視装置の構成を示すブロック図である。これは図１０の構成において、ネットワーク構成記録部１０３とネットワーク構成変化検出部１０４とを省略した構成である。このような構成にした場合、実施の形態１０の場合と比較して、ネットワーク構成が変化しない場合でも判断を行なわねばならず、判断部１０７の処理が多くなる一方、全体の構成が簡単になる。

【００８２】本発明の実施の形態１１におけるネットワーク監視装置を以上のように構成することにより、簡易な構成で、バスリセットにともなうネットワーク構成の変化を最小の手順で検出し、予め与えられた情報を基にネットワークに不正な機器の接続された可能性を自動的に検出できるネットワーク監視装置を実現することができる。

【００８３】（実施の形態１２）図１２は本発明の実施の形態１２におけるネットワーク監視方法の流れ図である。４２１はネットワーク構成検出手段を調査するフェイズ、４２２は使用できる全てのネットワーク検出手段を用いるフェイズ、４２３はネットワーク構成を検出するフェイズ、４２４は検出したネットワーク構成を記録するフェイズ、４２５は複数の手段から検出されたネットワーク構成に矛盾がないか比較するフェイズ、４２６はユーザに警告を行なうフェイズである。

【００８４】次に図１２を参照して、本発明の実施の形態１２におけるネットワーク監視方法を説明する。まず最初に、ネットワーク構成を検出する手段としてどのような手段が使用可能かについて調査を行なう（４２１）。４２１で得られたネットワーク構成検出手段を用いてネットワーク構成の検出を行なう（４２２）。各ネットワーク構成検出手段はネットワーク構成を検出し（４２３）、検出されたネットワーク構成は記録される（４２４）。なお、ここでは全てのネットワーク構成検出手段を用いることになっているが、指定された数、指定された時間、指定された手段、等実際にネットワーク構成を検出する手段を限定してもよい。検出された複数のネットワーク構成は、互いに矛盾がないか比較される（４２５）。矛盾が存在した場合、ネットワーク上に不正な機器が存在するか、機器あるいはネットワーク構成検出手段が故障している可能性があるため、ユーザに警告を行なう（４２６）。矛盾が存在しなかった場合、そのネットワーク構成は正しいものとされ出力される。複数のネットワーク構成検出手段で得られたネットワーク構成に矛盾があった場合、その情報を元に信用できないネットワーク構成検出手段を検出することができる。同様にしてネットワーク構成検出手段の故障を検出することができる。また、ネットワーク構成検出手段を複数持つことで、ネットワーク構成検出手段の故障に対して強靭となる。

【００８５】なお、４２６でユーザに警告を行なう場合、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００８６】本発明の実施の形態１２におけるネットワーク監視方法を以上のように実現することにより、ネットワーク構成獲得手段を複数持つことでフォールトトレランスを維持することができ、また、不正なトポロジマップを検出することでネットワークに不正な機器の接続された可能性を検出できるネットワーク監視方法を実現することができる。

【００８７】（実施の形態１３）図１３は本発明の実施の形態１３におけるネットワーク監視装置の構成を示すブロック図であり、図３に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図１３は図３におけるネットワーク構成検出部１０２の内部に実現する場合を示しており、１０２ａ～１０２ｘは複数存在するネットワーク構成検出手段であり、１０２ｙは検出されたネットワーク構成を記録する記録部であり、１０２ｚは複数の手段から検出されたネットワーク構成に矛盾がないか比較する比較部である。

【００８８】次に図１３を参照して、本発明における実施の形態１３におけるネットワーク監視装置の動作を説明する。ここで説明する実施の形態１３は、図３におけるネットワーク構成検出部１０２の内部に実現する場合について説明する。ネットワーク構成を検出する時刻になる、あるいは検出する指令を受けたネットワーク構成検出部はネットワーク構成の検出を行なう。複数のネットワーク構成検出手段１０２ａ～１０２ｘは、それぞれの手段でネットワーク構成を検出する。ネットワーク構成を獲得したネットワーク構成検出手段１０２ａ～１０２ｘは、ネットワーク構成を記録部１０２ｙに記録する。比較部１０２ｚは、記録部１０２ｙに記録された複数の検出手段に因るネットワーク構成を比較し、互いに矛盾がないかを調べる。矛盾が認められなかった場合、ネットワーク構成記録部１０３とネットワーク構成変化検出部１０４にネットワーク構成を出力する。矛盾が認められた場合、警告発生部１０８にその旨を出力する。複数のネットワーク構成検出手段で得られたネットワーク構成に矛盾があった場合、その情報を元に信用できないネットワーク構成検出手段を検出することができる。同様にしてネットワーク構成検出手段の故障を検出することができる。また、ネットワーク構成検出手段１０２ａ～１０２ｘを複数持つことで、ネットワーク構成検出手段の故障に対して強靭となる。

【００８９】本発明の実施の形態１３におけるネットワーク監視装置を以上のように構成することにより、ネッ

トワーク構成獲得手段を複数持つことでフォールトトレランスを維持することができ、また、不正なトポロジマップを検出することでネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。また、本発明の実施の形態１３におけるネットワーク監視装置のように、このネットワーク監視装置を他のネットワーク監視装置のネットワーク構成検出部として実装することも可能であり、それによってセキュリティレベルを上げることができる。

【００９０】（実施の形態１４）図１４は本発明の実施の形態１４におけるネットワーク監視方法の流れ図である。４３１は伝送遅延を測定するフェイズ、４３２は測定した伝送遅延を記録するフェイズ、４３３は伝送遅延を比較し、変化を検出するフェイズ、４３４はユーザに警告を出すフェイズである。

【００９１】次に図１４を参照して、本発明の実施の形態１４におけるネットワーク監視方法を説明する。監視者は設定された時刻にネットワーク上の伝送遅延時間を測定する（４３１）。測定時刻については、バスリセット直後、一定時間間隔、ランダム時間間隔、トラフィックの少ない時間、特定のイベントの直前または直後、ユーザの指示した時刻、常時、等の手段がある。測定手段としては、遅延測定用のパケットを測定対象ノードに送信しａｃｋを観察する、ネットワーク上を流れるリクエストパケットとそれに対するａｃｋを観察する、等の手段がある。測定された伝送遅延時間は記録される（４３２）。新たに記録された伝送遅延時間は、過去に記録された伝送遅延時間、または設定された伝送遅延時間と比較される（４３３）。比較した結果、伝送遅延時間の変化が認められない場合、４３１に戻り、次の伝送遅延測定時刻を待つ。伝送遅延の変化が認められる場合、ユーザに警告を行なう（４３４）。

【００９２】なお、４３４でユーザに警告を行なう場合、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００９３】本発明の実施の形態１４におけるネットワーク監視方法を以上のように実現することにより、伝送遅延を計測することができ、伝送遅延の変化からネットワークに不正な機器の接続された可能性を検出できるネットワーク監視方法を実現することができる。また、請求項１～２０に記載のネットワーク監視方法およびネットワーク監視装置とともに用いることにより、ネットワークをネットワーク構成とノード間の伝送遅延との二種類の情報から監視することが可能になり、ネットワークのセキュリティレベルを上げることができるという作用を有する。

【００９４】（実施の形態１５）図１５は本発明の実施の形態１５におけるネットワーク監視装置の構成を示すブロック図である。１０１はネットワーク、１２１は設定されたネットワーク機器の検出条件を記録する検出条件記録部、１２３は監視情報を記録しておく記録部、１２４は記録から伝達遅延の変化を検出する変化検出部、１２５は変化を検出した場合、警告を発する警告発生部である。１２６は遅延検査用のパケットを送信するパケット送信部であり、１２７は遅延検査用のパケットを受信するパケット受信部である。

【００９５】図１６は検出条件記録部１２１および記録部１２３で使用される記録テーブルの概念図である。１５１は機器毎の検出条件テーブルと応答結果記録テーブルを管理する機器テーブルであり、１５２は検出条件を記録する検出条件テーブルであり、１５３はパケットの送信時刻と機器からの応答のパケット受信時刻を記録する応答結果テーブルである。

【００９６】次に、図１５、１６を参照して、本発明の実施の形態１５におけるネットワーク監視装置の動作を説明する。最初にユーザは検出条件記録部１２１に検出条件を設定、記録する。パケット送信部１２６は、検索条件に従ってネットワーク機器へ遅延測定用のパケットを発信する。パケット受信部１２７は、機器から返ってきた遅延測定用パケットへの応答を受信する。監視したパケットは記録部１２３に記録される。変化検出部１２４は、記録部１２３の記録と検出条件記録部１２１の検出条件とから許容されない伝達遅延の変化があるかどうかを検出する。許容されない伝達遅延の変化が検出された場合、警告発生部１２５はユーザに警告を発する。

【００９７】なお、検出条件記録部１２１に設定、記録される検出条件は、検出時刻、時間、頻度、許容変化範囲、ホップ数、ケーブル長、中継機器などの経路の条件、特殊な機器の条件、機器の秘密共有鍵、機器の公開鍵、送信パケットの条件、機器についての情報などである。また、記録部１２３は、リクエストのパケットとそれに応じる応答パケットの間の時間を記録しても良く、またパケットのダンプ、パケットの一部、パケットの内容等も併せて記録しても良い。また、警告発生部１２５は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【００９８】本発明の実施の形態１５におけるネットワーク監視装置を以上のように構成することにより伝送遅延を計測することができ、伝送遅延の変化からネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。また、請求項１～２０に記載のネットワーク監視方法およびネットワーク監視装置とともに用いることにより、ネットワークをネットワーク構成とノード間の伝送遅延との二種類

の情報から監視することが可能になり、ネットワークのセキュリティレベルを上げることができる。

【００９９】（実施の形態１６）図１７は本発明の実施の形態１６におけるネットワーク監視装置の構成を示すブロック図である。１０１はネットワーク、１２１は設定されたネットワーク機器の検出条件を記録する検出条件記録部、１２２はネットワーク上のパケットを監視するパケット監視部、１２３は監視情報を記録しておく記録部、１２４は記録から伝達遅延の変化を検出する変化検出部、１２５は変化を検出した場合、警告を発する警告発生部である。

【０１００】図１８は記録部１２３で使用される記録テーブルの概念図である。１４１は機器間経路と応答時間記録テーブルとの関係を記録するテーブルであり、１４２は機器間の応答時間を記録するテーブルである。

【０１０１】次に、図１７、１８を参照して、本発明の実施の形態１６におけるネットワーク監視装置の動作を説明する。最初にユーザは検出条件記録部１２１に検出条件を設定、記録する。パケット監視部１２２は、検索条件に従ってパネットワーク上のパケットを監視し、監視したパケットは記録部１２３に記録される。図１８に示すように、監視は機器間の経路単位で行なわれ、リクエストのパケットとそれに応じる応答パケットの対がそれぞれ観測された時刻が記録される。変化検出部１２４は、記録部１２３の記録と検出条件記録部１２１の検出条件とから許容されない伝達遅延の変化があるかどうかを検出する。許容されない伝達遅延の変化が検出された場合、警告発生部１２５はユーザに警告を発する。

【０１０２】なお、検出条件記録部１２１に設定、記録される検出条件は、検出時刻、時間、頻度、検出するパケット、許容変化範囲、機器間経路のホップ数、ケーブル長、中継機器などの経路の条件、機器とネットワーク監視装置間経路ののホップ数、ケーブル長、中継機器などの経路の条件、特殊な機器の条件などである。また、記録部１２３は、リクエストのパケットとそれに応じる応答パケットの間の時間を記録しても良く、またパケットのダンプ、パケットの一部、パケットの内容等も併せて記録しても良い。また、警告発生部１２５は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【０１０３】本発明の実施の形態１６におけるネットワーク監視装置を以上のように構成することにより、ネットワークのトラフィックを増加させることなく簡易な構成で伝送遅延を計測することができ、伝送遅延の変化からネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。また、請求項１～２０に記載のネットワーク監視方法およびネットワーク監視装置とともに用いることにより、ネットワークをネットワーク構成とノード間の伝送遅延との二種類の情報から監視することが可能になり、ネットワークのセキュリティレベルを上げることができる。

【０１０４】（実施の形態１７）図１９は本発明の実施の形態１７におけるネットワークおよびネットワーク監視装置のふるまいの概念図である。２０１はネットワーク監視装置であり、２０２は監視対象のネットワーク機器である。２０３はネットワークがセキュアであることが確認されたことを示しており、２０４はネットワークにバスリセットがかかったことを示している。２０５はバスリセット前に予め交換しておくバスリセット前情報であり、２０６はバスリセット後に交換される認証情報要求であり、２０７は認証情報である。

【０１０５】本発明実施の形態１７におけるネットワークに接続されるネットワーク機器は、互いに情報を交換し、交換した情報を記録しておく能力を有する。ネットワーク上の機器はバスリセットが起こる前に予め情報を交換しておき、バスリセット後にその情報を用いることによりバスリセットに因われない運用が可能になる。例えば、バスリセット前に各機器の固有の名前または仮想的なＩＤと物理ＩＤとの組をバスリセット前に交換しておき、バスリセット後にも同様の情報を交換することで、バスリセットの前後で変化する各機器の物理ＩＤ変換テーブルを得ることができ、物理ＩＤに因われない運用が可能となり、また、ネットワーク構成の変化も知ることができる。

【０１０６】次に、図１９を参照して本発明の実施の形態１７におけるネットワークおよびネットワーク監視装置の動作の例を説明する。ここではバスリセット前に交換した情報をバスリセット後に秘密鍵として用いることで機器の承認を行なう。まず、セキュア確認２０３を経てネットワークのセキュリティが確認される必要がある。ここでネットワーク上に不正を働くネットワーク機器、悪意を実現することに利用できるネットワーク機器が存在しない状態であることが確認される。セキュアなネットワーク上の情報は秘密情報として扱うことができるため、ネットワーク監視装置２０１はこの時に鍵となるバスリセット前情報２０５をネットワーク機器２０２に送信する。この情報は予測されてはならないため、ここでは乱数を使ったことにする。この乱数を以後乱数Ａと呼ぶ。ネットワーク監視装置２０１およびネットワーク機器２０２は、このバスリセット前情報２０５を記憶しておく。

【０１０７】バスリセット２０４が起こると、それは新たな機器がネットワークに接続された可能性を示すために、これ以後はネットワークのセキュリティは保証されない。ここでバスリセット前情報２０５を利用してネットワーク機器２０２の認証を行なう。ネットワーク監視装置はバスリセット前情報２０５に含まれる情報、ここ

では乱数Ａを関数に通した値を、認証情報要求２０６と一緒にネットワーク機器２０２に送信する。ここでは関数としてハッシュ関数を用いている。この関数が、逆変換のできない、あるいは逆変換の困難な一方向関数である場合、この関数は公開されていてもよいが、少なくとも相手のネットワーク機器２０２はこの関数を知っている必要がある。ここではここでは乱数Ａを関数に通した値をHash( 乱数Ａ) とする。

【０１０８】認証情報要求を受けたネットワーク機器２０２は、バスリセット前情報と既知の関数から認証情報要求２０６に含まれるHash（乱数Ａ）を計算し、ネットワーク監視装置２０１がバスリセット前情報を交換したネットワークネットワーク監視装置であることを確認する。確認後、ネットワーク機器は、乱数Ａと自分のＩＤとのＸＯＲをとった値を関数に通した、Hash（乱数Ａ｜ＩＤ）およびＩＤを認証情報２０７としてネットワークネットワーク監視装置に送信する。ネットワーク機器が乱数ＡとＩＤとのＸＯＲをとるのは、認証情報２０７が認証確認情報２０６で鸚鵡返しできては困るためであり、既知の異なる関数を用いたり、ネットワーク監視装置２０１が認証情報要求２０６と共に塩を送りそれを利用したり、ＩＤの代わりに乱数などの適当な値を用いたりする、などの別の手段を用いてもよい。認証情報２０７を受信したネットワーク監視装置２０１は、乱数ＡとＩＤからHash（乱数Ａ｜ＩＤ）を計算し、ネットワーク機器２０２がバスリセット前情報を交換したネットワーク機器であることを確認できる。このプロセスを全ての機器に行なうことでバスリセット前から接続されていた機器の認証を行なうことができる。このプロセスは、なりすましを防止するために機器毎に行なった方が良い。具体的にはバスリセット前情報２０５の乱数を機器毎に変えると良い。

【０１０９】本発明の実施の形態１７におけるネットワークおよびネットワーク監視装置を以上のように構成することにより、バスリセット前に交換した情報をバスリセット後に利用することができるネットワークを得ることができる。また、バスリセット前情報を以上のように利用することで、バスリセット以前から存在する機器の認証を行なうことができるネットワークおよびネットワーク監視装置を得ることができる。

【０１１０】（実施の形態１８）図２０は本発明の実施の形態１８におけるネットワーク監視装置およびネットワーク機器の構成を示すブロック図である。１０１はネットワークであり、１６１はネットワーク監視装置である。ネットワーク監視装置１６１において、１６２は送受信部であり、１６３は機器認証処理を行なう機器認証処理部であり、１６４は記録部であり、１６５は鍵生成部であり、１６６はバスリセット検出部である。１７１はネットワーク機器であり、１７２はネットワーク機器の送受信部であり、１７３はネットワーク機器の機器認証処理部であり、１７４はネットワーク機器の記録部である。

【０１１１】次に、図２０を参照して、本発明の実施の形態１８におけるネットワーク監視装置およびネットワーク機器の動作を説明する。ネットワークがセキュアであることが確認できた後、ネットワーク監視装置１６１の鍵生成部１６５は、認証用の鍵を生成する。鍵は送受信部１６２を通して伝送され、また伝送先の情報とともに記録部１６４に記録される。ネットワーク機器１７１は、送受信部１７２で鍵を受信し、記録部１７４に記録する。

【０１１２】バスリセットが発生すると、バスリセット検出部１６６がそれを検出し、機器認証処理部１６３に通知する。機器認証処理部１６３は、記録部１６４に記録されている鍵を用いてネットワーク機器の認証のための情報を生成し、送受信部１６２を通してネットワーク機器１７１に伝送される。ネットワーク機器１７１は送受信部１７２で認証情報を受信する。それを受けて、機器認証処理部１７３は受信した認証情報および記録部１７４に記録されている鍵を用いて認証情報を生成し、送受信部１７２を通してネットワーク監視装置１６１に送信する。ネットワーク監視装置１６１の認証処理部１６３は、送受信部１６２を介して認証情報を受信し、機器の認証を行なう。

【０１１３】ここではネットワーク監視装置１６１がバスリセットを関知し、他のネットワーク機器の認証のトリガとなる情報を生成する例を挙げているが、ネットワーク機器がそれぞれバスリセットを関知し認証情報を生成しても良い。また、ネットワーク機器が鍵を生成しても良い。また、認証を一回の応答で行なっているが、セキュアのために複数回の応答が必要な認証を行なっても良い。なお、バスリセット前の情報として、鍵以外にも、現在のネットワーク構成、次に起こることが想定されるネットワーク構成の変化、などを交換することもできる。

【０１１４】本発明の実施の形態１８におけるネットワーク監視装置およびネットワーク機器を以上のように構成することにより、バスリセット前に交換した情報をバスリセット後に利用することができるネットワーク監視装置およびネットワーク機器を得ることができる。また、バスリセット前情報を以上のように利用することで、バスリセット以前から存在する機器の認証を行なうことができるネットワーク監視装置およびネットワーク機器を得ることができる。

【０１１５】（実施の形態１９）図２１は本発明の実施の形態１９における監視システムの構成例を示すブロック図である。３０１はカメラ、３０２はマイク、３０３はセンサ、３０４は表示装置、３０５は記録装置、３０６はバスブリッジ、３０７はユーザ端末、３０８は請求項１～２６に記載のネットワーク監視方法を具備した機

器あるいはネットワーク監視装置である。

【０１１６】次に、図２１を参照して本発明の実施の形態１９における監視システムの動作を説明する。最初にユーザはユーザ端末３０７から設定項目をネットワーク監視装置３０８に入力する。次にネットワーク監視装置３０８は、ネットワーク構成情報を取得し、ネットワーク構成が許容されているものであるかどうかを判断し、許容されていない場合にはユーザに警告を行なう。また、ネットワーク監視装置３０８は、ネットワーク上の伝送遅延を調査し、伝送遅延の変化が許容されているものかどうかを判断し、許容されていない場合にはユーザに警告を行なう。また、ネットワークが許容される状態である時はセキュアであると判断し、ネットワーク監視装置３０８は、予め秘密鍵となる情報をネットワーク機器３０１～３０６と交換しておく。バスリセットの発生は、ネットワーク構成の変化の可能性を意味するため、少なくともバスリセット毎にネットワーク監視装置３０８はネットワーク構成および伝送遅延を取得し、許容されているものであるかどうかを調査する。

【０１１７】警告が出された場合、それはネットワークが設定で許されていない状態に変化したことを意味する。ユーザは警告を受け、現在の状態を警告に付随する情報を利用し調査を行なう。その結果、その状態もセキュアであるとユーザが判断した場合、ユーザ端末３０７を通してその旨をネットワーク監視装置３０８に伝える。ネットワーク監視装置３０８はその状態を許容される状態として蓄積する。

【０１１８】本発明の実施の形態１９における監視システムを以上のように構成することにより、ネットワークに接続しようとする不正な機器を発見し、ネットワークをセキュアに保つことができるネットワーク監視システムを得ることができる。

【０１１９】

【発明の効果】以上のように、本発明によれば、ネットワーク構成を監視することにより、ネットワークへの機器の追加、削除およびネットワーク構成の変化を検出し、ネットワークへの不正な機器の接続を発見することができるネットワーク監視装置を得ることができる。また、伝送遅延を監視することによりネットワークへの機器の追加、削除およびネットワーク構成の変化を検出し、ネットワークへの不正な機器の接続を発見することができるネットワーク監視装置を得ることができる。また、バスリセット前に情報を交換しておくことによりバスリセット前から接続されている機器の認証を行ない、ネットワークへの機器の追加、削除およびネットワーク構成の変化を検出し、ネットワークへの不正な機器の接続を発見することができるネットワーク監視装置を得ることができる。また、ネットワーク自体をセキュアに保つことのできるネットワーク監視システムを得ることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１におけるネットワーク監視方法を説明する概念図

【図２】本発明の実施の形態２におけるネットワーク監視方法の構成を示す流れ図

【図３】本発明の実施の形態３におけるネットワーク監視装置の構成を示すブロック図

【図４】本発明の実施の形態４におけるネットワーク監視方法の構成を示す流れ図

【図５】本発明の実施の形態５におけるネットワーク監視装置の構成を示すブロック図

【図６】本発明の実施の形態６におけるネットワーク監視装置の構成を示すブロック図

【図７】本発明の実施の形態７におけるネットワーク監視方法の構成を示す流れ図

【図８】本発明の実施の形態８におけるネットワーク監視装置の構成を示すブロック図

【図９】本発明の実施の形態９におけるネットワーク監視方法の構成を示す流れ図

【図１０】本発明の実施の形態１０におけるネットワーク監視装置の構成を示すブロック図

【図１１】本発明の実施の形態１１におけるネットワーク監視装置の構成を示すブロック図

【図１２】本発明の実施の形態１２におけるネットワーク監視方法の構成を示す流れ図

【図１３】本発明の実施の形態１３におけるネットワーク監視装置の構成を示すブロック図

【図１４】本発明の実施の形態１４におけるネットワーク監視方法の構成を示す流れ図

【図１５】本発明の実施の形態１５におけるネットワーク監視装置の構成を示すブロック図

【図１６】本発明の実施の形態１５におけるネットワーク監視装置の監視記録テーブルの概念図

【図１７】本発明の実施の形態１６におけるネットワーク監視装置の構成を示すブロック図

【図１８】本発明の実施の形態１６におけるネットワーク監視装置の監視条件、記録テーブルの概念図

【図１９】本発明の実施の形態１７におけるネットワーク監視方法の概念図

【図２０】本発明の実施の形態１８におけるネットワーク監視装置のブロック図

【図２１】本発明の実施の形態１９における監視システムの概念図

【符号の説明】

１０１　ネットワーク

１０２　ネットワーク構成検出部

１０２ａ～１０２ｘ　ネットワーク構成検出手段

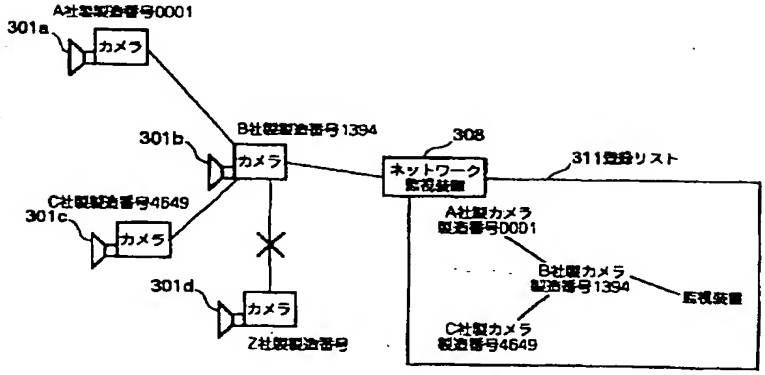
１０２ｙ　記録部

１０２ｚ　比較部

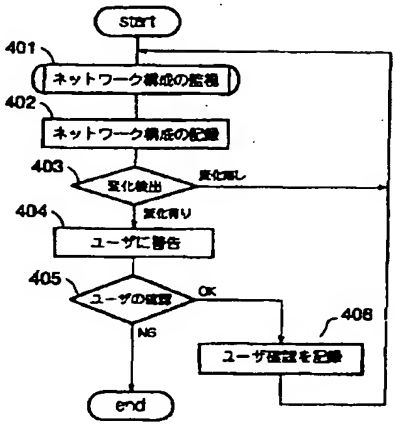
１０３　ネットワーク構成記録部

１０４　ネットワーク構成変化検出部
１０５　表示部
１０６　許容ネットワーク構成記録部
１０７　判断部
１０８　警告発生部
１０９　バスリセット検出部
１１０　入力部
１２１　検出条件記録部
１２２　パケット監視部
１２３　記録部
１２４　変化検出部
１２５　警告発生部
１２６　パケット送信部
１２７　パケット受信部
１４１　経路テーブル
１４２　応答時間記録テーブル
１５１　機器確認テーブル
１５２　検出条件テーブル
１５３　応答結果記録テーブル
１６１　ネットワーク監視装置
１６２　送受信部
１６３　機器認証処理部
１６４　記録部
１６５　鍵生成部
１６６　バスリセット検出部
１７１　ネットワーク機器
１７２　送受信部
１７３　機器認証処理部
１７４　記録部
２０１　ネットワーク監視装置
２０２　ネットワーク機器
２０３　セキュア確認
２０４　バスリセット
２０５　バスリセット前情報
２０６　認証情報要求
２０７　認証情報
３０１　カメラ
３０２　マイク
３０３　センサ
３０４　表示装置
３０５　記録装置
３０６　バスブリッジ
３０７　ユーザ端末
３０８　ネットワーク監視装置
３１１　登録リスト

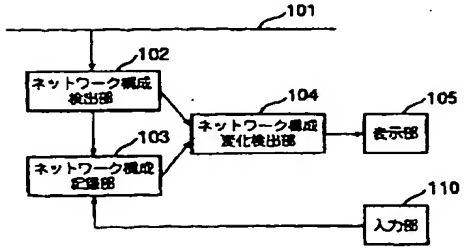
【図１】



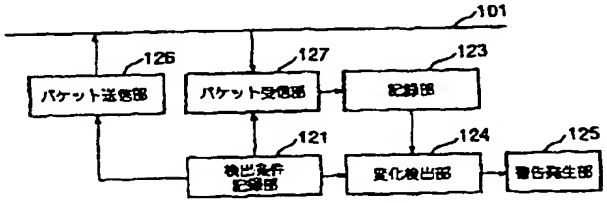

【図２】




【図３】

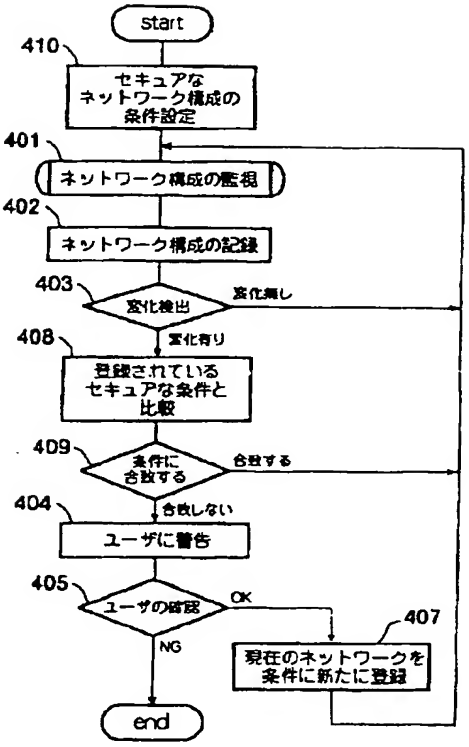



【図１５】

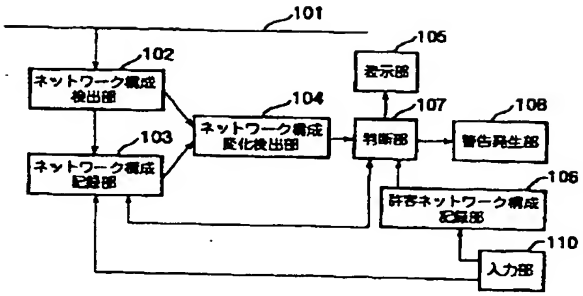


【図４】

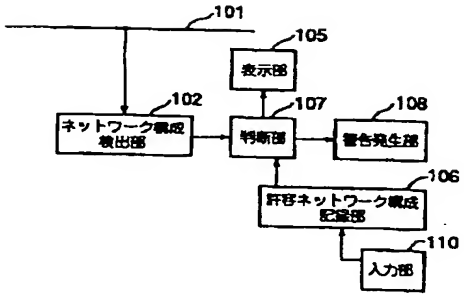



start
410
セキュアな
ネットワーク構成の
条件設定
401
ネットワーク構成の監視
402
ネットワーク構成の記録
403
変化検出
変化無し
変化有り
408
登録されている
セキュアな条件と
比較
409
条件に
合致する
合致する
合致しない
404
ユーザに警告
405
ユーザの確認
OK
NG
407
現在のネットワークを
条件に新たに登録
end

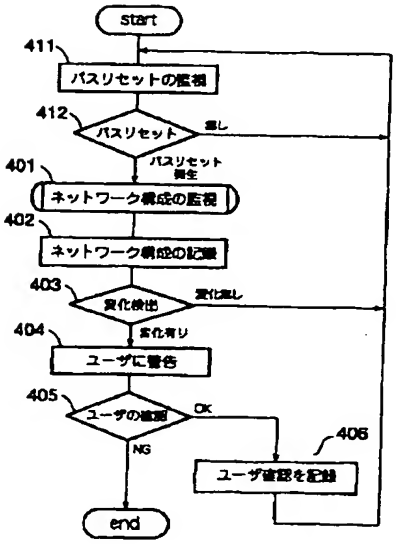
【図５】



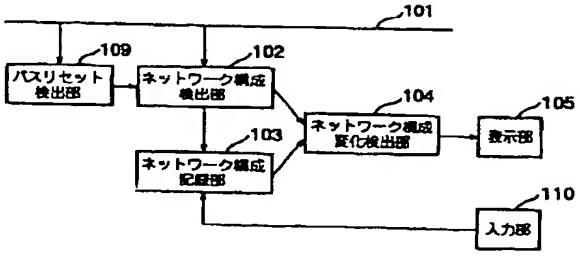

【図６】



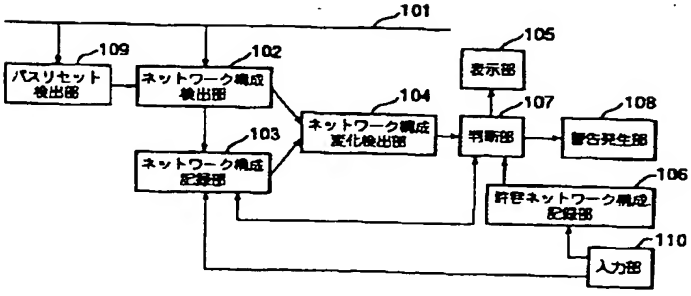

【図７】



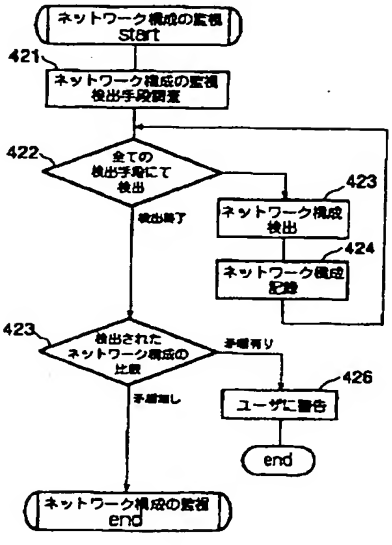

【図８】



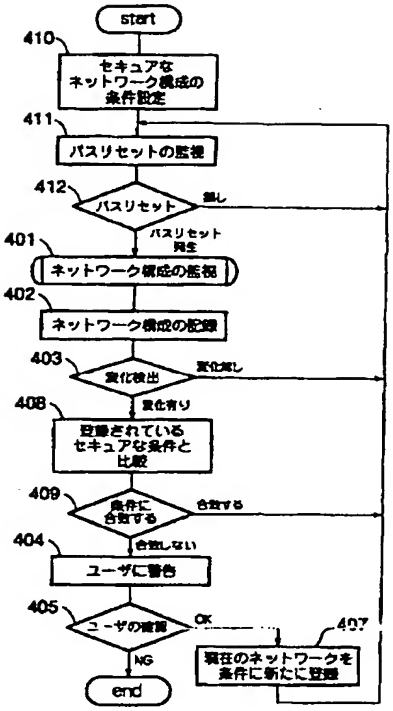

【図１０】



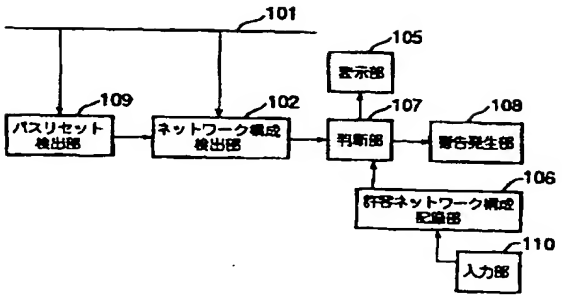

【図１２】



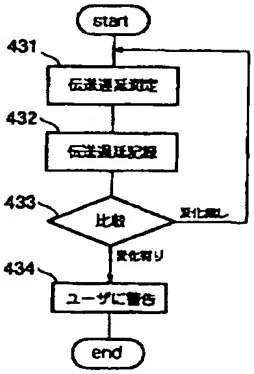
【図９】



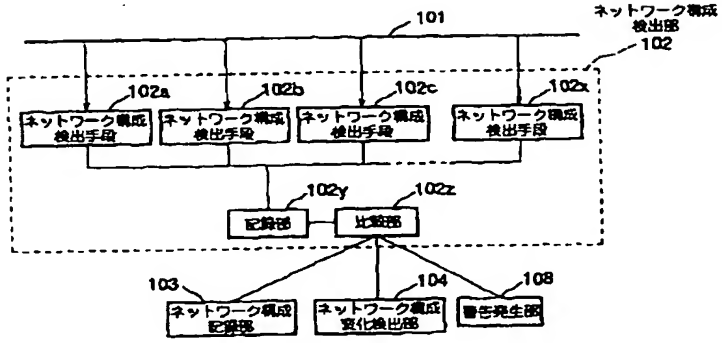

【図１１】



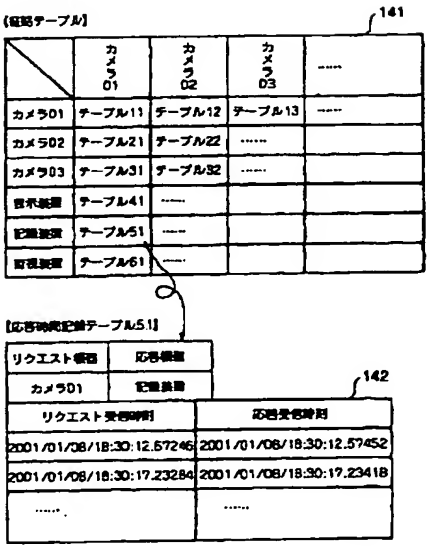

【図１４】




【図１３】




【図１８】

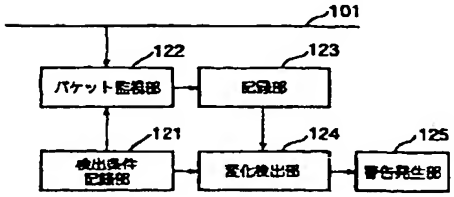



| | カメラ01 | カメラ02 | カメラ03 | ..... |
|---|---|---|---|---|
| カメラ01 | テーブル11 | テーブル12 | テーブル13 | ..... |
| カメラ02 | テーブル21 | テーブル22 | ..... | |
| カメラ03 | テーブル31 | テーブル32 | ..... | |
| 表示装置 | テーブル41 | ..... | | |
| 記録装置 | テーブル51 | ..... | | |
| 監視装置 | テーブル61 | ..... | | |

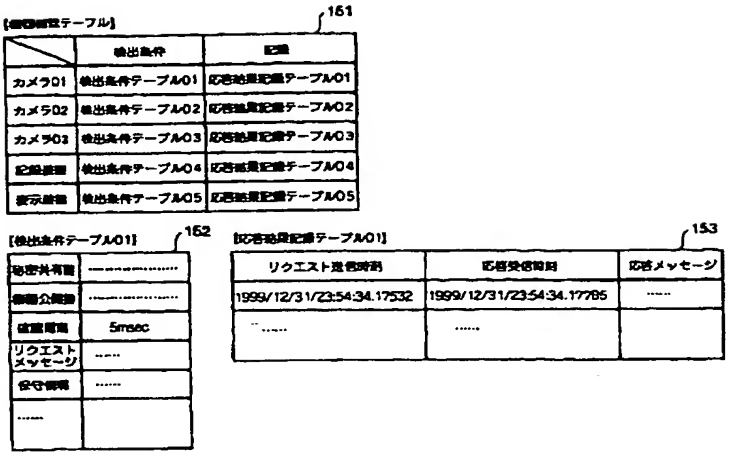
| リクエスト種別 | 応答種別 |
|---|---|
| カメラ01 | 記録装置 |

| リクエスト受信時刻 | 応答送信時刻 |
|---|---|
| 2001/01/08/18:30:12.57245 | 2001/01/08/18:30:12.57452 |
| 2001/01/08/18:30:17.23284 | 2001/01/08/18:30:17.23418 |
| ..... | ..... |

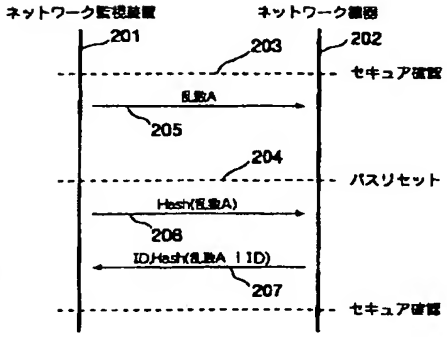
【図１７】



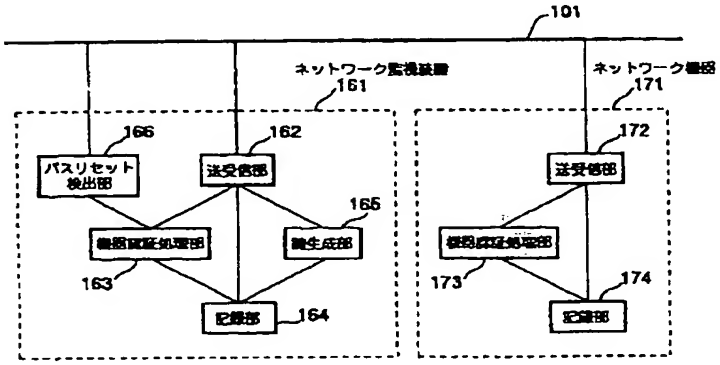
【図１６】



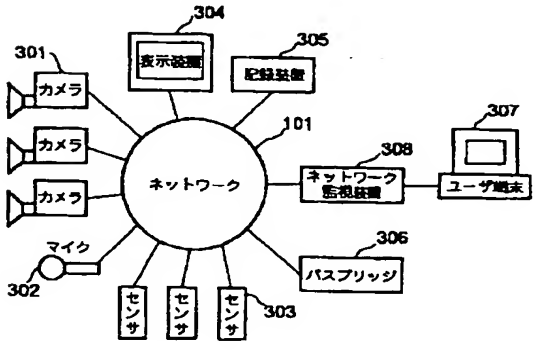

【図１９】




【図２０】




【図２１】



フロントページの続き

(72)発明者 都築 健吾
神奈川県横浜市港北区綱島東四丁目３番１号 松下通信工業株式会社内

Ｆターム(参考) 5K030 GA15 HB08 HC13 JT04 MA01
MA06 MD07 MD08
5K033 AA08 BA01 BA08 DA01 DA16
DB20 EA03